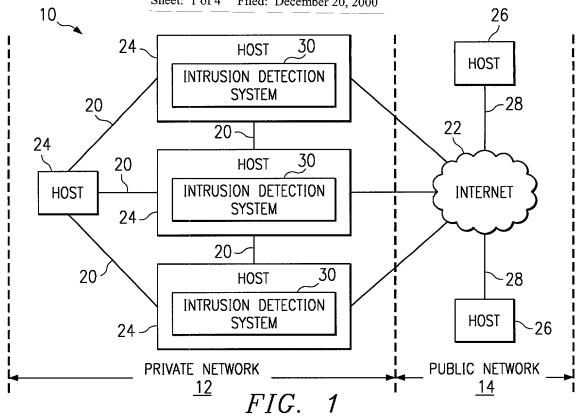
Method and System for Maintaining Network Activity Data for Intrusion Detection

Inventor: Wiley, et al.

Attorney's Docket: 062891.0424

Sheet: 1 of 4 Filed: December 20, 2000



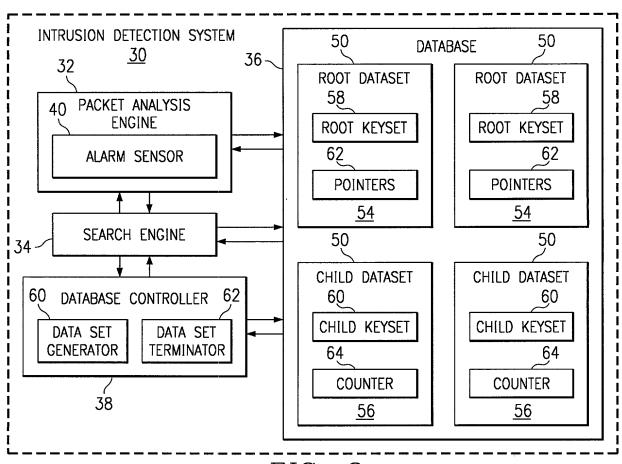
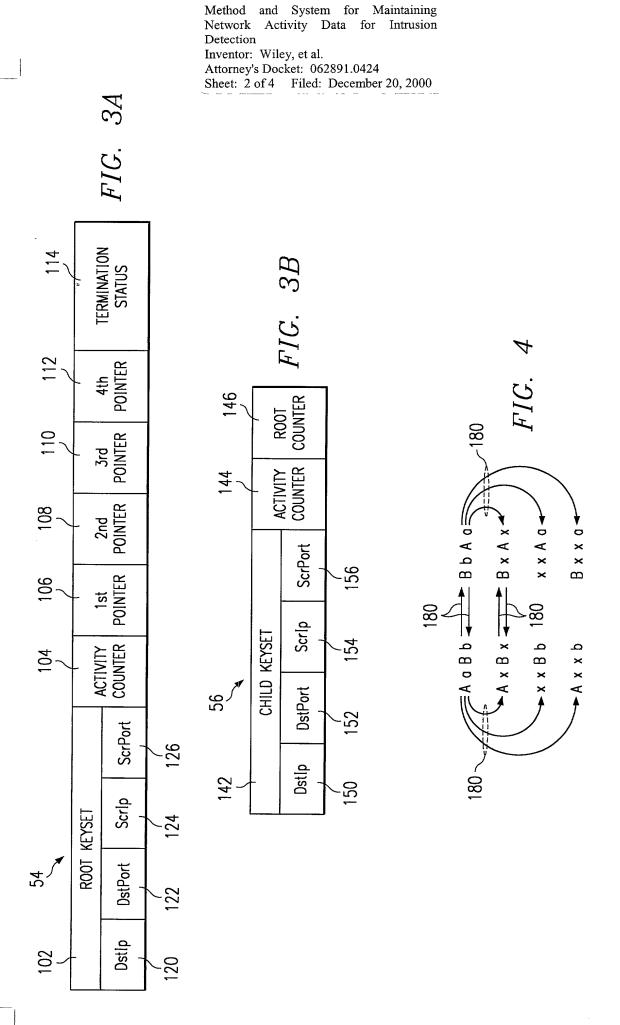


FIG. 2



Attorney's Docket: 062891.0424 Sheet: 3 of 4 Filed: December 20, 2000 **START** IDENTIFY TRAFFIC 200-SIGNATURE FOR INTRUSION DETECTION PROCESSING FIG. 5 SEARCH NETWORK ACTIVITY 202-DATA FOR NEXT DATASET CORRESPONDING TO SIGNATURE 204 **ROOT** YES DATASET EXIST? 222 NO, 206 GENERATE ROOT DATASET IDENTIFY ROOT DATASET 208-SEARCH NETWORK ACTIVITY IDENTIFY SIBLING AND CHILD DATA FOR SIBLING DATASET DATASETS FROM ROOT DATASET 224 210 RETRIEVE DATA FROM ROOT, SIBLING CHILD, SIBLING AND KEY YES -226 DATASET DATASETS FOR SIGNATURE EXIST? COMPARE DATA TO NO, INTRUSION DETECTION 228 GENERATE SIBLING DATASET LIMITS THRESHOLDS SEARCH NETWORK ACTIVITY ATTACK NO 214-DATA FOR DATASETS **UNDERWAY?** 216 230 YES. ALL CHILD YES **ALARM** 232 DATASETS **EXIST? END** ,NO GENERATE ABSENT CHILD 218-DATASETS ASSOCIATE ROOT, SIBLING 220 AND CHILD DATASETS

Method and System for Maintaining Network Activity Data for Intrusion

Detection

Inventor: Wiley, et al.

Method and System for Maintaining Network Activity Data for Intrusion

Detection

Inventor: Wiley, et al.

Attorney's Docket: 062891.0424

Sheet: 4 of 4 Filed: December 20, 2000

